



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,463	04/18/2001	Rouslan Beletski	47-12 US	8867

25319 7590 10/06/2004

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER

TRUONG, THANHNGA B

ART UNIT PAPER NUMBER

2135

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/836,463	Applicant(s) BELETSKI, ROUSLAN	
	Examiner Thanhnga Truong	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Eldridge et al (US 6,515,988).

a. Referring to claim 1:

i. Eldridge teaches:

(1) a display for displaying data to be digitally signed [i.e., the portable device is preferably a handheld or wristwatch computer with a graphical display for enabling the user to transfer tokens, and the fixed devices preferably include a scanner/copier/printer having its own IR transceiver, wherein the token contains a string or icon which can be displayed to identify the document or service to which the token refers for the benefit of the user (column 2, lines 40-42 and abstract)];

(2) a transducer for receiving the user authorization information and for providing user authorization data based thereon [i.e., the security information includes a digital signature of the information in the token. The digital signature is a digest of information in the token and its encryption with the document owner's private key. These signatures can only be generated by the personal portable device since only it has the private key. The signature ensures the integrity of the token and attests that the token did originate from a known portable device (column 2, lines 47-56)]; and

(3) a processor for providing data based on an electronic document for digitally being signed to the display in a secure fashion such that the displayed data is known to be based upon the electronic document, for receiving the user authorization data, for verifying the user authorization data against stored template data, and for digitally signing the electronic document upon determining that the user authorization data is provided from an authorized user [i.e., accordingly, Eldridge's invention provides a method for supporting a wide range of digital applications that can be carried out in a data processing device that includes a processor, memory, and a user interface. In response to user input, the data processing device can generate a token comprising an operation component designating a document related operation (e.g. single sided or double sided print command), an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service. This token is transmitted to another device (e.g. the network printer), which can check security, parameters, and modify its default operations in response to user input to the data processing device (column 1, lines 50-67)],

(4) wherein the processor provides the data based on the electronic document to the display for review prior to digitally signing the electronic document [i.e., referring to Figure 3A, the components (32, 34, 342, 344, 36, 38, 382-389) of the general form of the satchel token 30 are schematically illustrated. All the components (32, 34, 342, 344, 36, 38, 382-389) taken together form a Satchel Token general 30. They are stored inside a user's PDA 2 (but they can also be stored in user's personal computers/workstations) as small packets having the structure indicated in FIG. 3. They are taken out of this form and linearised (made into a straight linear sequence of ASCII characters) when needed. This can be done for two reasons: (i) so that a token can be transported through some communications medium (wired or wireless) and (ii) so that the

token as a whole can be taken as a linear sequence of ASCII characters for secure hashing and then digital signing operations to form the token's digital signature component (column 6, lines 33-47)].

b. Referring to claim 2:

i. Eldridge further teaches:

(1) wherein the display, the transducer, and the processor are disposed within a same secure housing [i.e., **Figures 5 and 6 show a portable computing device which includes a display, a processor, user authentication, and user interface**].

c. Referring to claim 3:

i. Eldridge further teaches:

(1) wherein the secure housing forms part of a personal digital assistant housing [i.e., **Figure 2 shows a portable computing device, such as personal digital assistants (PDAs), handheld PCs, or pocket or wristwatch computers (column 5, lines 26-28)**].

d. Referring to claims 4, 5, 13, 14, 15, and 16:

i. These claims have limitations that is similar to those of claim 1 (4), thus they are rejected with the same rationale applied against claim 1 (4) above.

e. Referring to claims 6, 7, and 8:

i. These claims have limitations that is similar to those of claim 1 (2), thus they are rejected with the same rationale applied against claim 1 (2) above.

f. Referring to claim 9:

i. Eldridge further teaches:

(1) non-volatile storage including executable instructions stored therein for performing functions associated with a personal digital assistant [i.e., **data processing device that includes a processor, memory (that is a “non-volatile storage”), and a user interface (column 1, lines 52-53)**].

g. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

h. Referring to claim 11:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

i. Referring to claims 12 and 18:

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

j. Referring to claim 17:

i. Eldridge teaches:

(1) providing the electronic document to a secure processor [i.e., tokens which include security information are presented to "secure documents servers" (column 3, lines 11-12)];

(2) displaying data based on the electronic document, the data provided from the processor to a display along a secure communication path therebetween [i.e., accordingly, the present invention provides a method for supporting a wide range of digital applications that can be carried out in a data processing device that includes a processor, memory, and a user interface. In response to user input, the data processing device can generate a token comprising an operation component designating a document related operation (e.g. single sided or double sided print command), an address component designating the electronic address of a document or system providing a document related service, one or more parameter components, each parameter component defining a property of a document or a property of a service to be applied to a document, and a security parameter dependent upon the identity of a user associated with a document or with a document related service. This token is transmitted to another device (e.g. the network printer), which can check security, parameters, and modify its default operations in response to user input to the data processing device (column 1, lines 50-67)];

(3) receiving authorization data [i.e., each portable device is in effect a user's personal satchel for documents, with the devices being programmed to receive, transmit, and store document identifiers (e.g. World Wide

Web URLs), each of which is associated with an electronic document stored in an electronic repository at a site on the web (column 1, lines 29-35)]; and

(4) when the authorization data is indicative of an authorization to digitally sign the displayed data, digitally signing the electronic document to provide a signed document [i.e., referring to **Figure 3A**, the components (32, 34, 342, 344, 36, 38, 382-389) of the general form of the satchel token 30 are schematically illustrated. All the components (32, 34, 342, 344, 36, 38, 382-389) taken together form a Satchel Token general 30. They are stored inside a user's PDA 2 (but they can also be stored in user's personal computers/workstations) as small packets having the structure indicated in FIG. 3. They are taken out of this form and linearised (made into a straight linear sequence of ASCII characters) when needed. This can be done for two reasons: (i) so that a token can be transported through some communications medium (wired or wireless) and (ii) so that the token as a whole can be taken as a linear sequence of ASCII characters for secure hashing and then digital signing operations to form the token's digital signature component (column 6, lines 33-47)].

k. Referring to claim 19:

i. This claim has limitations that is similar to those of claim 1 (3), thus it is rejected with the same rationale applied against claim 1 (3) above.

l. Referring to claim 20:

i. This claim has limitations that is similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

m. Referring to claim 21:

i. Eldridge further teaches:

(1) wherein any instructions in execution on the processor is secure software that is verified by a secure entity [i.e., a secure server contains a "gatekeeper" which verifies signatures on tokens and examines the specified conditions associated with the token and then acts accordingly (e.g. encrypting the document with the appropriate key) (column 3, lines 12-16)].

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 1, 11, and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Smithies et al (US 5,818,955).

a. Referring to claim 1:

i. Smithies teaches:

(1) a display for displaying data to be digitally signed [i.e., the client application presents the required information to a signature capture module 4 (also called a signature capture service), which in turn requests that a user sign his or her signature using the appropriate hardware devices, such as, for example, a combination of a pen/digitizer and display 8 (column 7, lines 38-42)];

(2) a transducer for receiving the user authorization information and for providing user authorization data based thereon [i.e., the signature capture module 4 and the signature verification module 6 utilize a set of APIs (Application Program Interfaces) to permit the incorporation of signature capture and verification into many different applications, e.g., 2a and 2b. Applications can determine the context for each signature and the criteria for signature verification thresholds. (column 8, lines 8-13)]; and

(3) a processor for providing data based on an electronic document for digitally being signed to the display in a secure fashion such that the displayed data is known to be based upon the electronic document, for receiving the user authorization data, for verifying the user authorization data against stored template data, and for digitally signing the electronic document upon determining that the user authorization data is provided from an authorized user [i.e., in the representative

embodiment, the signature capture module 4 requires the availability both of a graphical display device and a digitizer. Under both Windows for Pen Computing and Pen for OS/2, any graphical display device supported by the operating system may be used, for example, Wacom, Calcomp, Kurta, etc. In addition, the computer processor can be any pen-based computer supporting either of these operating systems, such as, for example, Compaq's Concerto computer or IBM's P-Series Thinkpad computer (column 8, lines 22-31)],

(4) wherein the processor provides the data based on the electronic document to the display for review prior to digitally signing the electronic document [i.e., referring to Figure 3A, the client application 2 may supply to the signature capture module 4 an identification of the document being signed and/or the reason why (or importance of) the document being signed. This information is the gravity prompt 22. In the representative embodiment, the gravity prompt 22 is displayed to the user in the signature capture window 20. This allows the user to make sure that the document being signed is the one that the user believes he or she is signing, and moreover, alerts the user to reason for and the gravity of the act of signing (column 10, lines 57-66)].

b. Referring to claim 11:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

c. Referring to claim 17:

i. Smithies teaches:

(1) providing the electronic document to a secure processor [i.e., the signature capture module encrypts data representing, inter alia, the act-of-signing statistics, the time and date of signing, the claimed identity of the signer, the words that appear in the gravity prompt, the document checksum, and optionally, data representing a graphic image of the signature. The signature capture module creates a signature envelope that comprises this encrypted data. In the representative embodiment, the signature envelope is an

encrypted string of data. Accordingly, the signature envelope is a secure way to represent the inscription event (column 4, lines 52-61)];

(2) displaying data based on the electronic document, the data provided from the processor to a display along a secure communication path therebetween [i.e., the client application presents the required information to a **signature capture module 4 (also called a signature capture service)**, which in turn requests that a user sign his or her signature using the appropriate hardware devices, such as, for example, a combination of a pen/digitizer and display 8 (column 7, lines 38-42). The signature verification module and template database may be located at a remote location, accessible by many client applications. For example, the signature verification module and template database may be located at a central independent signature verification bureau. In an alternative embodiment, the signature verification module and template database are located upon the local system, accessible by the client application when necessary (column 5, lines 6-15)];

(3) receiving authorization data [i.e., signature capture module is for capturing and/or receiving a handwritten signature(see Figure 1)]; and

(4) when the authorization data is indicative of an authorization to digitally sign the displayed data, digitally signing the electronic document to provide a signed document [i.e., referring to Figure 3A, the client application 2 may supply to the signature capture module 4 an identification of the document being signed and/or the reason why (or importance of) the document being signed. This information is the gravity prompt 22. In the representative embodiment, the gravity prompt 22 is displayed to the user in the signature capture window 20. This allows the user to make sure that the document being signed is the one that the user believes he or she is signing, and moreover, alerts the user to reason for and the gravity of the act of signing (column 10, lines 57-66)].

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Beard (US 5, 867, 821) discloses a method and apparatus for transaction verification is provided. An acoustic signature of a transaction executioner is captured and electronically saved as a digital signature file. (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

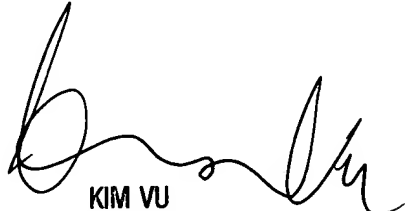
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TC 2100 will be moved to Carlyle in October 2004, the new telephone number for TC 2100 receptionist is 571-272-2100. In October 2004, any inquiry concerning this communication should be directed to Thanhnga (Tanya) Truong whose new telephone number is 571-272-3858, and the examiner's supervisor, Kim Vu can be reached at 571-272-3859.

TBT

September 28, 2004


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER